SPYWOLF

Security Audit Report

Completed on

April 4, 2023

OVERVIEW

This audit has been prepared for **Padmon DAO** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

Padmon DAO

PROJECT DESCRIPTION

According to their whitepaper:

PadmonDAO is a DAO-styled launchpad platform established on BSC network that allows for our community to be able to directly take part in the full process of project research and determination of which projects are brought on to our platform for their early presale raises.

There will be proposals brought to the community in which summaries of info for upcoming projects are provided along with all relevant links. The community is given a predetermined amount of time to read over the project details and then cast their vote on which they would like to participate in investing in!

Release Date: Presale starts in April, 2023

Category: DAO

CONTRACT INFO

Token Name
PadmonDAO

Symbol
PDAO

Contract Address
0x55139a7687cd0cfd888c8ff612A8919Fa6DfC7B0

Network
Binance Smart Chain

Language
Solidity

Deployment Date
Apr 03, 2023

Verified?
Yes

Total Supply
50,000,000

Status
Not launched

TAXES

Buy Tax
8%

Sell Tax
11%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	17
Uniq Senders	6
Uniq Receivers	6
Total Amount	80002720 PDAO
Median Transfer Amount	10 PDAO
Average Transfer Amount	4706042.352941176 PDAO
First transfer date	2023-04-03
Last transfer date	2023-04-03
Days token transferred	1

SMART CONTRACT STATS

Calls Count	28
External calls	13
Internal calls	15
Transactions count	26
Uniq Callers	6
Days contract called	1
Last transaction time	2023-04-03 15:16:29 UTC
Created	2023-04-03 11:30:47 UTC
Create TX	0x5d2bcd682d2b637f73cde8db4760f8f64d48a7e46bf458590ca8bfbc545b6646
Creator	0x76d887ef073c240cc090bcd1c87dc75552341f53

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

Owner can change swapTokensAtAmount which is responsible to autoswap accumulated tokens from fees.
If swapTokensAtAmount is set to 0, selling will fail for all users.

```
function setSwapTokensAtAmount(uint256 amount) external onlyOwner {
    swapTokensAtAmount = amount;
}
```

- Recommendation:
  - Ensure that swapTokensAtAmount variable is always above 1 token, considering also token's decimals.

FOUND THREATS

⚠ High Risk

Owner can blacklist address.
For blacklisted addresses it is impossible to buy or sell.
If the liquidity pair is blacklisted, the trading will halt for all users.

```
function blacklistAddress(address account, bool value) external onlyOwner{
    _isBlacklisted[account] = value;
}
```

- Recommendation:
  - Ensure that the liquidity pair is always excluded from such restrictions.

FOUND THREATS

⚠ Medium Risk

Owner can set buy/sell fees up to 20%.
Combined buy+sell = 40%.
When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make.
Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.

```
function setPurchaseFee(uint256 _newlpfee, uint256 _newmarketingfee, uint256 _newcharityfee) public onlyOwner {
    require((_newlpfee + _newmarketingfee + _newcharityfee) <= maxFeePercent,"Fee exceed the maximum limit");
    purchaseLPFee = _newlpfee;
    purchaseMarketingFee = _newmarketingfee;
    purchaseCharityFee = _newcharityfee;
}
function setSellFee(uint256 _newlpfee, uint256 _newmarketingfee, uint256 _newcharityfee) public onlyOwner {
    require((_newlpfee + _newmarketingfee + _newcharityfee) <= maxFeePercent,"Fee exceed the maximum limit");
    sellLPFee = _newlpfee;
    sellMarketingFee = _newmarketingfee;
    sellCharityFee = _newcharityfee;
}
```

- Recommendation:
  - Considered as good tax deduction practice is buy and sell fees combined not to exceed 25%.

FOUND THREATS

⚠ Low Risk

No low risk-level threats found in this contract.

Informational

Owner can set max transaction and max wallet amount but cannot lower it than 0.01% of total supply. When transaction limitations are applied, users will be subject to transfer restrictions up to certain amounts (depending on current setting).

```
function setMaxTxAmount(uint256 _amount) external onlyOwner {
    require(_amount > 5000 ether, "Zero: Max transaction amount can't be 0!");
    maxTxAmount = _amount;
}
function setMaxWalletAmount(uint256 _amount) external onlyOwner() {
    require(_amount > 5000 ether, "Zero: Max wallet amount can't be 0!");
    maxWalletAmount = _amount;
}
```

Owner can exclude address from limits.
Limits such as max wallet and max transaction will not apply to excluded address.

```
function excludeFromLimits(address account, bool excluded) public onlyOwner {
    require(_isExcludedFromLimits[account] != excluded, "Account is already the value of 'excluded'");
    _isExcludedFromLimits[account] = excluded;
    emit ExcludeFromLimits(account, excluded);
}

function excludeMultipleAccountsFromLimits(address[] memory accounts, bool excluded) public onlyOwner {
    for(uint256 i = 0; i < accounts.length; i++) {
        _isExcludedFromLimits[accounts[i]] = excluded;
    }
    emit ExcludeMultipleAccountsFromLimits(accounts, excluded);
}
```

Informational

Owner can withdraw any tokens from the contract with exception of the native PDAO token.
When this function is present, in cases tokens sent into the contract by mistake or purposefully, contract's owner can retrieve them.

```
function retrieveStuckTokens(address tokenaddress, address recipient, uint amount) external onlyOwner {
    require(tokenaddress != address(this),"Not retrieve native tokens!");
    require(amount <= IERC20(tokenaddress).balanceOf(address(this)),
    "Insufficient balance to transfer the requested amount.");
    super._transfer(address(this), recipient, amount);
}
function retrieveStuckBnb(address recipient, uint amount) external onlyOwner {
    require(amount <= address(this).balance, "Insufficient balance to transfer the requested amount.");
    (bool success, ) = payable(recipient).call{ value: amount }("");
    require(success, "Address: unable to extract value");
}
```

Owner can exclude address from fees.
When address is excluded from fees, the user will receive the whole amount of the bought, sold and/or transferred tokens.

```
function excludeFromFees(address account, bool excluded) public onlyOwner {
    require(_isExcludedFromFees[account] != excluded, "Account is already the value of 'excluded'");
    _isExcludedFromFees[account] = excluded;
    emit ExcludeFromFees(account, excluded);
}

function excludeMultipleAccountsFromFees(address[] memory accounts, bool excluded) public onlyOwner {
    for(uint256 i = 0; i < accounts.length; i++) {
        _isExcludedFromFees[accounts[i]] = excluded;
    }
    emit ExcludeMultipleAccountsFromFees(accounts, excluded);
}
```

Informational

IMPORTANT

Trading restriction based on tradingOpen variable will niot apply, because the liquidity pair is already excluded from limits.

```
constructor() ERC20("PadmonDAO", "PDAO") {
.......................
_isExcludedFromLimits[uniswapV2Pair] = true;
.......................
}

function _transfer(
address from,
address to,
uint256 amount
) internal override {
.......................
if (from != owner()) {

    if(!_isExcludedFromLimits[from] && !_isExcludedFromLimits[to]){
        require(tradingOpen,"Trading not open yet");
    }
}
.......................
}
```

Replacement code fix example:

```
if (from != owner()) {
    if (to == uniswapV2Pair && !_isExcludedFromLimits[from]) {
    require(tradingOpen,"Trading not open yet");
    } else if(from == uniswapV2Pair && !_isExcludedFromLimits[to]) {
    require(tradingOpen,"Trading not open yet");
    }
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

Padmon DAO

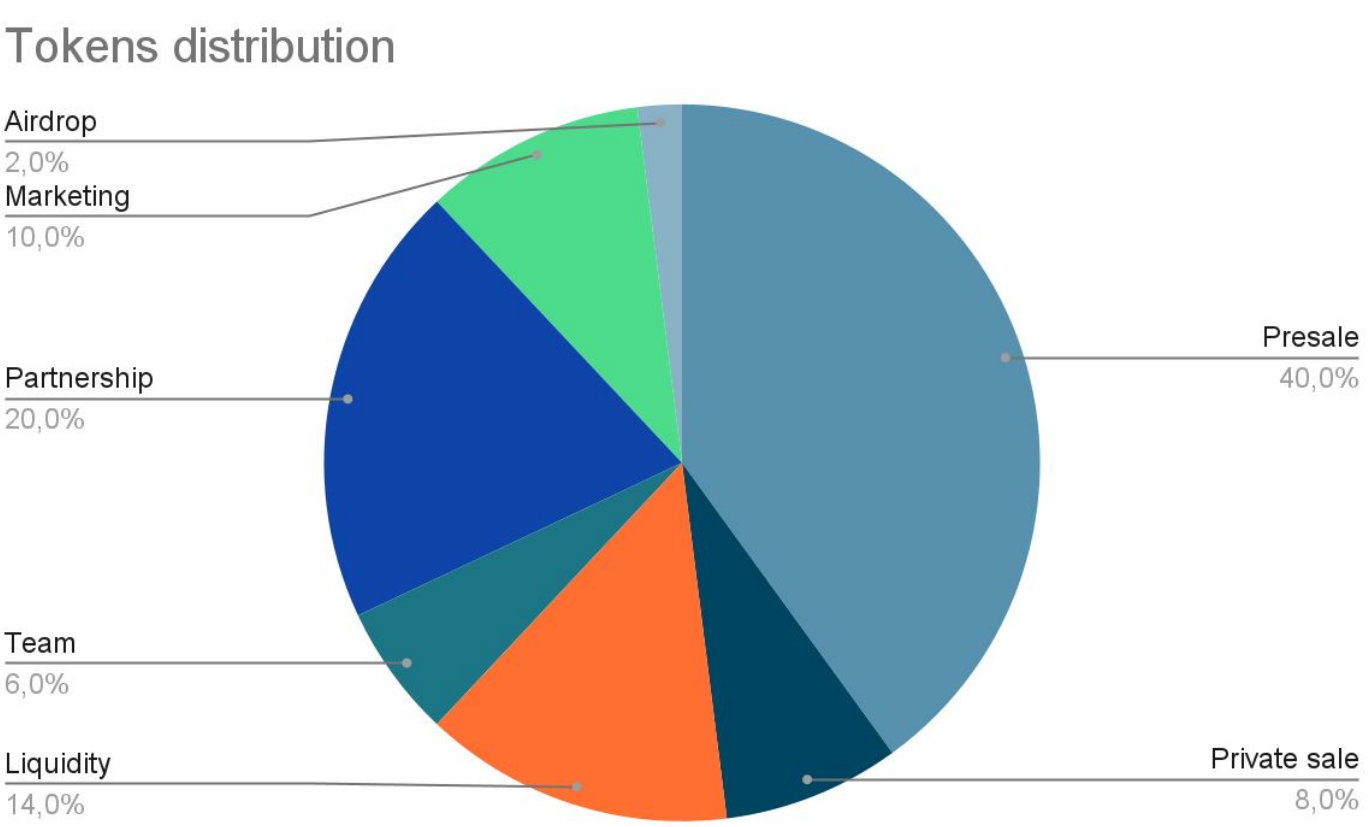
GOOD PRACTICES FOUND

- ✔ The owner cannot mint new tokens after deployment
- ✔ The owner can set a transaction limit, but can’t lower it than 0.01% of total supply

TOKENOMICS

The following tokenomics are based on the project's whitepaper and/or website:

- 8% - Private sale
- 40% - Presale
- 14% - Liquidity
- 6% - Team
- 20% - Partnership
- 10% - Marketing
- 2% - Airdrop



For more information about vesting periods check project’s whitepaper:
https://padmondao.gitbook.io/padmon/usdpdao-token/tokenomics

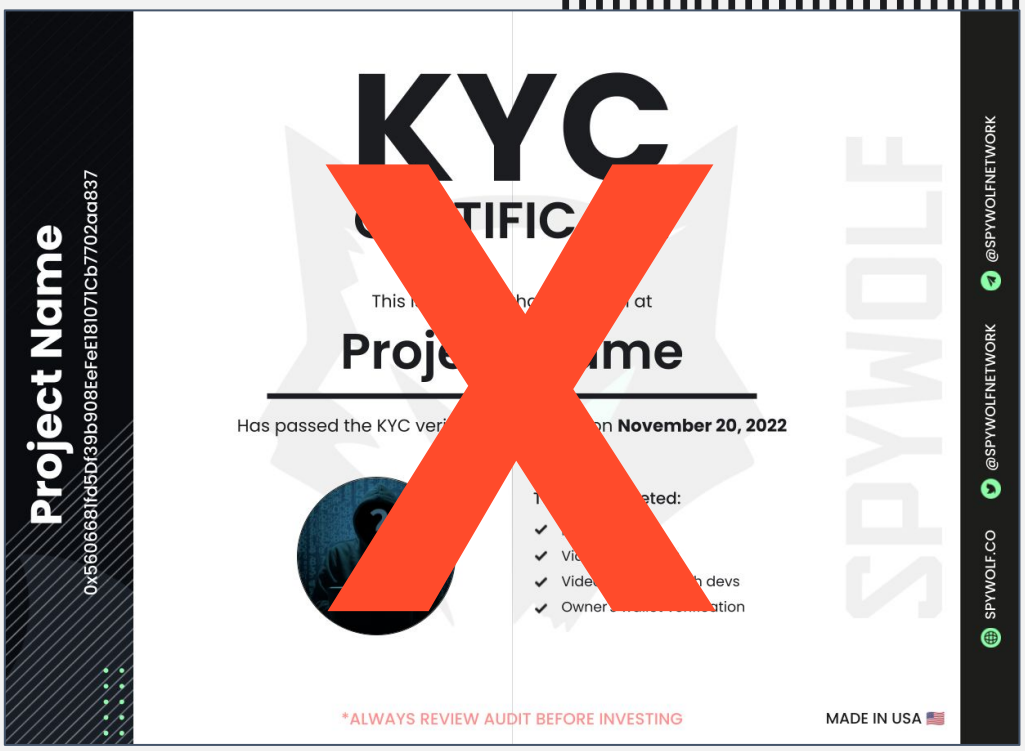
THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

⚠️ No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



WEBSITE

Website URL
https://www.padmon.io/

Domain Registry
https://www.namecheap.com/

Domain Expiration
2023-12-01

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
Single page design with appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
Well written, explanatory.

Roadmap
Yes, goals set without time frames.

Mobile-friendly?
Yes

padmon.io

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media pages are active with many members.

Twitter

@PadmonDAO

- 17 600 followers
- Very active
- Posts frequently

Discord

https://discord.com/invite/m7rStPVyGG

- 58 members
- Few active members
- Active mods

Telegram

@TelegramUSERNAME

- 2 889 members
- Active members
- Active mods

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 400 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.